Sent by email to:
JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

23 January 2018

**Response to draft *Guidelines on Transparency under Regulation 2016/679***

Dear Sir or Madam,

Thank you for the opportunity to respond to the draft Guidelines on Transparency. This is a joint submission from UK Finance and the Association for Financial Markets in Europe (AFME).[1]

Our annexed response focuses in the first instance on the importance of getting the balance right between providing detailed information on the one hand, and maximising data subject engagement and interest in privacy matters on the other. This is followed by several more specific technical suggestions.

We would be happy to discuss further with you and to answer any questions you may have.

Yours faithfully,


Walter McCahon

Policy manager
**UK Finance**
T +44 20 3934 1131| M +44 7 725 683263
E walter.mccahon@ukfinance.org.uk

Richard Middleton

Managing Director
**AFME**
T +44 20 3828 2709 | M +44 7584 583 122
E richard.middleton@afme.eu


[1] AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society. AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is registered on the EU Transparency Register, registration number 65110063986-76.

UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

**Primary issue – finding the balance between detail and data subject engagement**

Transparency is an important protection for data subjects, as recognised in the GDPR particularly under Articles 12, 13 and 14. Data subjects have a right to understand how their personal data are being processed.

The challenge when trying to ensure transparency is to explain what will sometimes be complex processing operations in a manner that data subjects will understand. Similarly, information relating to personal data processing needs to be provided in a manner that data subjects will engage with rather than ignore. Controllers need to minimise 'information fatigue' whereby data subjects mechanically click through privacy notices without reading them or throw away unread hard copy letters.

Given the amount of information that must be provided under the GDPR text, meeting this challenge will not always be straightforward. The draft guidelines recognise this important balancing act, in particular by recommending a 'layered approach' to the provision of privacy information. We agree that this is a helpful tool.

However, there are also areas of the guidance which require, or recommend as best practice, the provision of information which is not required by the GDPR text itself. However, in our view, the information set out under Articles 13 and 14 already provide data subjects with a good picture of the processing.

We recognise that there may be some merit in providing certain additional information beyond what is set out in Articles 13 and 14 in some situations and that there is an important overarching requirement of fairness and transparency that firms should consider. However, providing more information will not *necessarily* be the best way to ensure these outcomes or to protect data subjects. Data subjects' ability and willingness to review the total amount of information they receive also needs to be considered, along with the impact on the overall risk of data subject information fatigue.

Similarly, the more information provided, the more often data controllers will need to send updates to data subjects. If data subjects receive too many notifications of privacy notice updates, there is a risk that they will lose interest and disengage from privacy issues.

In our view there is therefore a risk that adding additional information beyond what is required in Articles 13 and 14 will in fact hinder data subjects' understanding and engagement without providing substantive additional protection, particularly if the information in question will frequently need to be updated.

We outline the specific areas of concern below.

<u>Paragraph 40 – explaining 'compatibility analysis'</u>

- Although we can understand the principle behind explaining this assessment to data subjects, we note that this is not a requirement of Articles 13 and 14.
- These assessments will necessarily be legalistic and would need to cover a range of considerations, given the content of Article 6(4). A description of the assessment would therefore probably be relatively lengthy and complex.
- Providing this information risks increasing information fatigue among data subjects. As such, we question whether this additional information would be beneficial overall for data subjects.

- We recommend that this paragraph be revised along the lines of:

  *"WP29's position is that in adherence to the principle of transparency expressed in Article 12 and the essential requisites of accountability and fairness under the GDPR, data controllers should* ***consider*** *provid* ***ing*** *data subjects with further information on the compatibility analysis carried out under Article 6.4,* ***or making this available on request****…"*

Paragraph 41 – "reasonable period"

- The draft guidelines state: "*What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects*."
- It would be useful for the final guidelines to include some examples of appropriate timeframes for providing updated transparency information.

Page 31 – information on the 'balancing of interests'

- The 'balancing of interests' requirement when controllers wish to rely on 'legitimate interests' is an important protection for data subjects.
- However, the exact calculation done by the controller does not need to be provided to data subjects under the GDPR text.
- As with the 'compatibility analysis', this balancing exercise is likely to be quite technical. Similarly, data subjects want to know how their data is being collected and used but it is unlikely they will understand what a 'balancing of interests test' is or why they ought to read it.
- As such, providing this information risks causing data subjects to disengage from reading the privacy notice and would not in our view be 'best practice'.
- **We recommend** that this be revised along the lines of:
  *"…As a matter of best practice, the data controller should* ***consider whether it would be helpful to*** *also provide the data subject with the information from the balancing test…"*

Page 32 – recipients of the personal data

- We understand and agree with the objective of ensuring that data subjects understand how their personal data will be shared. Clearly it is important to know, for example, that personal data will be shared with third parties for marketing purposes.
- However, we think it unlikely that data subjects will in many cases be interested in the exact individual companies that will receive the data. In particular, we note that our members will often each engage hundreds of vendors (processors). Providing a list of hundreds of companies would increase the risk that data subjects disengage from the privacy notices.
- Furthermore, these vendors change frequently. If the controller has provided a list of named vendors as a part of its compliance with Articles 13(1)(e) and 14(1)(e), it will need to send updated information to data subjects each time there is a change of vendor. This would certainly lead to data subject 'information fatigue' and distract data subjects from more material updates to privacy information.
- In accordance with the principle of fairness and the wording of Articles 13(1)(e) and 14(1)(e), an appropriate description of the categories of recipient will be more meaningful for data subjects and more likely to engage their attention, while reducing the risk of information fatigue.

- **We recommend** that the guidelines be amended such that naming every individual recipient is no longer the 'default position'.

Page 33 – transfers to third countries

- In accordance with Article 13(1)(f) and 14(1)(f), we agree that controllers should disclose the Chapter V safeguards in place / whether there is an applicable adequacy decision.
- However, data subjects are unlikely to be interested in the specific article numbers from the GDPR. Including this information is likely to make a privacy notice appear more 'legalistic' and become less engaging and readable as a result.
- **We recommend** removing the recommendation to list the specific GDPR articles.
- Similarly, we are concerned that listing all of the third countries to which personal data might be transferred will increase the length and complexity of privacy notices and cause data subjects to be less engaged.
- As outlined in our earlier comments, we note that for a global organisation engaging many processors, it is likely that the exact third countries receiving personal data will change relatively frequently, including when a processor moves its operations. Contacting data subjects each time is likely to increase information fatigue and data subject disengagement from privacy information.
- The GDPR sets up a framework of safeguards for controllers to use to ensure that appropriate levels of data protection are achieved. This framework should be trusted. Advising customers, for example, that the storage of customer records is moving from India to South Africa is unlikely to provide significant additional protection, provided that the relevant transfers remain within a BCR, model contract framework or other valid safeguards.
- **We recommend** amending this paragraph to the effect of:
  "*…In accordance with the principle of fairness,* ***data controllers should consider whether it would help data subject understanding to*** ~~*the information should*~~ ***also*** *explicitly mention all third countries to which the data will be transferred."*

Page 33 – storage periods

- We agree with the principle that data subjects should understand how long their personal data will be held. However, providing more detail about retention periods might be counterproductive to data subject understanding.
- In the field of financial services, firms must hold personal data for a range of purposes, including a wide range of legal and regulatory compliance purposes. In this context, firms will hold many different types of personal data, with a range of different retention periods. Their retention schedules will therefore be complex.
- Furthermore, there are likely to be many caveats and exemptions to broad policies, depending on changes to regulation, requests and investigations by regulators, relevant legal action, etc.
- Explaining storage periods at a granular level of detail, as suggested in the draft guidelines, risks being less clear than a more general explanation, and could confuse the data subject or cause him/her to skip past the information.
- In our view, a more general approach would better inform data subjects, and achieve a higher level of engagement and understanding. For example, firms could explain the maximum amount of time that their personal data would be held for (for example, for financial services firms in the UK this would likely be the length of the relationship plus seven years, in accordance with anti-money laundering rules). Firms could then offer to provide the full retention policy on demand.
- **We recommend** removing the requirement to specify the exact retention period / policy for each data type and allowing a more flexible approach.

Page 35 – sources of data

- It is clearly important to provide an informative description of data sources to data subjects but specifying each individual source risks data subject information fatigue.
- Similar to other comments above, if every individual source is named in a privacy notice, the controller will have to notify data subjects each time there is a change. Controllers will often source data from many other firms, meaning that data subjects would likely receive large numbers of update notifications. Again, this risks increasing information fatigue and data subject disengagement.
- A description of the types of data sources used, along with an option to request the exact list if desired, would strike a better balance by providing useful information and access to detail where individuals are interested, while minimising the risk of information overload and potential disengagement by data subjects.
- **We recommend** that a description of *types* of sources should be permitted under the guidelines.

## Additional comments

Paragraph 9 on describing the consequences of processing:

- This paragraph arguably suggests that the controller should explain what might go wrong with the data processing. In particular, by stating that the description should not solely set out 'best case' examples, it could be inferred that the controller should explain theoretical 'worst case' scenarios. However, we do not think this is WP29's intention.
- **We recommend clarifying** that the explanation of the consequences of the processing should relate to the *intended* processing, rather than describing hypothetical scenarios about what might conceivably go wrong.
- For example: an explanation of pre-loan credit checks should indicate that the data subject might be refused a loan on the basis of the check and that a record will be kept of the fact that the individual has made a credit application. An explanation of what might happen in the event of a personal data breach would not need to be provided.
- WP29 might like to use this, or similar examples, to illustrate the interpretation of 'most important consequences'.

Paragraph 11 and example on 'Clear and plain language':

- It is unclear how this piece of guidance interacts with the 'layered approach'. In our view, statements similar to those in the example *would* be appropriate in the *first layer* of a privacy notice, provided the data subject can easily find the details in a second layer. In our view this is an appropriate technique for quickly drawing data subjects' attention to the high-level issues and giving ready access to the detail if the wish to access it.
- **We recommend** clarifying that broad statements / descriptions can be used in the first layer of a privacy notice, provided adequate detail is provided in subsequent layers.

Paragraph 22 on making sure that privacy statement updates are noticed

- This paragraph states "…the controller should take all measures necessary to ensure that [changes to the privacy notice] are communicated in such a way that ensures that most recipients will actually notice them."
- It would be useful to have some examples of how this could be achieved. For example:
    - Providing to the data subject a summary of the key changes and issues with a link to the online version of the full updated privacy statement and information about how to contact the controller if they have any questions or concerns.

- Including a flag in email signatures to indicate to recipients that the firm's privacy notice has been amended.
- In the context of a website privacy notice being updated, where the controller does not have contact details of those accessing the website, it should be adequate to keep the privacy notice up to date, with the date of the latest changes noted.

Paragraphs 43 – 45 – use of icons

- We note that in paragraph 45, WP29 states that it will need to do extensive research and consultation to inform icon design, and emphasises that universal recognition will be important. We agree with these points.
- If icons are to be adopted by industry, it is important that firms have confidence as to their meaning so that they can ensure consistency with their written privacy notices.

ENDS